

STATE OF ALABAMA

Information Technology Baseline

Baseline 660-02B1_Rev A: Server Security

1. INTRODUCTION:

Though operating system vendors have taken steps to make their operating system baseline configurations more secure on a default installation, additional operating system hardening efforts are usually required to enhance the confidentiality, integrity, and availability of the data present on the servers and accountability in regards to persons authorized access to the servers as well as complete restriction of unauthorized access. Furthermore, dependent on server functionality (e.g., domain controllers or Web servers) additional hardening must be considered based on the server's level of exposure to cyber threats. In order to reduce the exposure of State of Alabama server-based computing resources to cyber-related threats and unauthorized access, secure operating system baseline configurations are necessary as a fundamental countermeasure.

2. OBJECTIVE:

Define standard configuration settings for a secure operating system computing baseline for State of Alabama server computing resources.

3. SCOPE:

These requirements apply to all State of Alabama servers with specific requirements for those servers utilizing Microsoft Windows Server 2003 and Windows Server 2008.

4. REQUIREMENTS:

The following requirements, based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-123: Guide to General Server Security, apply to State of Alabama servers.

4.1 GENERAL SERVER SECURITY

Physical Security: Place servers in secured areas with controlled access. Additional physical security requirements are stated in State IT Standard 650-01S1: Physical Security.

Server Software: Install only the services required for the server and eliminate any known vulnerabilities through patches or upgrades. Any unnecessary applications, services, or scripts that are installed should be removed immediately once the installation process is complete. During the installation of the server software, the following steps should be performed:

- Install the server software either on a dedicated host or on a dedicated guest operating system (OS) if virtualization is being employed.
- Apply any patches or upgrades to correct for known vulnerabilities in the server software.

- Create a dedicated physical disk or logical partition (separate from OS and server application) for server data, if applicable.
- Remove or disable all services installed by the server application but not required (e.g., gopher, FTP, HTTP, remote administration).
- Remove or disable all unneeded default user accounts created by the server installation.
- Remove all manufacturers' documentation from the server.
- Remove all example or test files from the server, including sample content, scripts, and executable code.
- Remove all unneeded compilers.
- Apply the appropriate security template or hardening script to the server.
- Configure each network service to listen for client connections on only the necessary TCP and UDP ports, if possible.

Consider installing the server with non-standard directory names, directory locations, and filenames if possible. Many server attack tools and worms targeting servers only look for files and directories in their default locations. While this will not stop determined attackers, it will force them to work harder to compromise the server, and it also increases the likelihood of attack detection because of the failed attempts to access the default filenames and directories and the additional time needed to perform an attack.

4.2 SYSTEM-SPECIFIC SECURITY SETTINGS

To determine the specific security settings to use, organizations will first need to determine the server's role (domain controller, file server, Web server, etc.) and the appropriate operating environment (Legacy Client, Enterprise Client, or Specialized Security – Limited Functionality (SSLF)) based on the client types supported and/or the need for tighter security.

Document the designated operating environment and server role in system security plans and local operating procedures.

4.2.1 Windows Server 2003

NIST and the National Security Agency (NSA) recommend that Windows 2003 servers be configured in accordance with the guidelines published by Microsoft Corporation. The Microsoft publication, Windows Server 2003 Security Guide, provides the baseline configuration to be implemented on all State of Alabama servers running the Windows Server 2003 operating system.

Download the Windows Server 2003 Security Guide from the Microsoft Download Center: <http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en>

4.2.2 Windows Server 2008

The Microsoft publication, Windows Server 2008 Security Guide, provides the baseline configuration to be implemented on all State of Alabama servers running the Windows Server 2008 operating system.

Download the Windows Server 2008 Security Guide from the Microsoft Download Center: <http://www.microsoft.com/downloads/details.aspx?FamilyID=fb8b981f-227c-4af6-a44b-b115696a80ac&DisplayLang=en>

4.3 MAINTAINING SERVER SECURITY

After initially deploying a server, administrators need to maintain its security continuously. Securely administering a server on a daily basis is an essential aspect of server security. Maintaining the security of a server requires the following actions:

- Configuring, protecting, and analyzing log files in accordance with the requirements of State IT Standard 670-06S1: Log Management.
- Backing up critical information in accordance with the requirements of State IT Standard 670-07S1: Backup and Recovery.
- Establishing and following procedures for recovering from server compromise (refer to incident response procedures 600-04P1: Incident Reporting and 600-04P2: Incident Handling).
- Routinely and proactively updating systems with fixes, patches, definitions, and service packs in accordance with the requirements of State IT Standard 670-03S1: Vulnerability Management and organizational vulnerability management program(s).
- Testing security periodically.

5. DEFINITIONS:

ENTERPRISE CLIENT: Environment consisting of an Active Directory® domain with member servers and domain controllers that run Windows Server 2003/2008 and client computers running Windows 2000 and newer OS.

LEGACY CLIENT: Environment consisting of an Active Directory® directory service domain with member servers and domain controllers that run Windows Server 2003/2008 and some client computers that run Microsoft Windows 98 and Windows NT® 4.0. Computers running Windows 98 must have the Active Directory Client Extension (DSClient) installed.

SSLF: The SSLF environment consists of an Active Directory domain with member servers and domain controllers that run Windows Server 2003/2008 and clients that run Windows 2000 and newer OS. The SSLF security settings in Microsoft's "Windows Server 2003 Security Guide" track closely with the security level historically represented in the guidelines offered by NSA, NIST, and the security community. However, the SSLF settings are so restrictive that many applications may not function. This may affect server performance and make it more of a challenge to manage the servers. Also, client computers that are not secured by the SSLF policies could experience communication problems with client computers and servers that are secured by the SSLF policies.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 660-02: System Security

6.2 RELATED DOCUMENTS

Information Technology Procedure 600-04P1: Incident Reporting

Information Technology Procedure 600-04P2: Incident Handling

Information Technology Standard 650-01S1: Physical Security

Information Technology Standard 670-03S1: Vulnerability Management

Information Technology Standard 670-06S1: Log Management

Information Technology Standard 670-07S1: Backup and Recovery

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	12/18/2007	
Rev A	9/18/2008	Added general security requirements from NIST 800-123 and Windows Server 2008 Security Guide reference.